2. Polynomial rings

Let R be a ring. A polynomial in one variable over R is

$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, $a_i \in R$, x is a "variable" that can be "assigned" values from R or a subring $S \subseteq R$.

Formalize: Let $P(R)$ denote the set of sequences

$a = (a_i) = (a_0, a_1, a_2, \dots)$ where $a_i \in R$ and $a_i = 0$ for all but finitely many i. If $a, b \in P(R)$, define operations:

$$a + b = (a_i + b_i)$$
$$ab = \left(\sum_{j=0}^{i} a_j b_{i-j}\right) = (a_0 b_0,\ a_0 b_1 + a_1 b_0,\ a_0 b_2 + a_1 b_1 + a_2 b_0, \dots)$$

Thm 2.1: If R is a ring, then $P(R)$ is a ring. It is commutative iff R is, and it has 1 iff R does, in which case $1_{P(R)} = (1_R, 0, 0, 0, \dots)$

Pf: Exercise.

Let R be a ring with 1, set $x = (0, 1, 0, 0, \dots) \in P(R)$.

Note: $x^2 = (0, 0, 1, 0, 0, \dots)$, $x^3 = (0, 0, 0, 1, 0, 0, \dots)$, etc.

Say $x^0 = 1_{P(R)}$. The map $a \longmapsto (a, 0, 0, \dots)$ is a monom. $R \longrightarrow P(R)$. Thus we may identify R with a subring of $P(R)$, $1_R = 1_{P(R)}$. Now, we may write

$$a = (a_0, a_1, a_2, \dots) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots \quad \text{for each } a \in P(R).$$

Call x an indeterminate, and write $R[x] = P(R)$.

Write $f(x)$ for $a \in R[x]$, called a <u>polynomial</u> with coefficients in R. If $a_n \neq 0$, but $a_m = 0$ for all $m > n$, say $f(x)$ has <u>degree</u> n, and <u>leading coefficient</u> a_n. If $f(x)$ has leading coefficient 1, call $f(x)$ <u>monic</u>. Call the zero polynomial $(0,0,0,\ldots)$, denoted by 0. Say $\deg 0 = -\infty$.

Polynomials of degree 0 or $-\infty$ are <u>constants</u> (elts of R).

<u>Prop 2.2</u>: Let R be a ring with 1 & $f(x), g(x) \in R[x]$. Then

(a) $\deg(f(x)+g(x)) \leq \max\{\deg f(x), \deg g(x)\}$, and

(b) $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$.

Moreover, equality holds in (b) if R has no zero divisors.

<u>Pf</u>: Exercise

<u>Cor 1</u>: If R has no zero divisors, then $f(x) \in R[x]$ is a unit iff $f(x) = r$ with $r \in \mathcal{U}(R)$.

<u>Cor 2</u>: $R[x]$ is an integral domain iff R is an integral domain.

<u>Thm 2.3</u>: (Division algorithm). Suppose R is commutative with 1 and $f(x), g(x) \in R[x]$. If $g(x)$ has leading coeff. b, then there exists $k \geq 0$ and $q(x), r(x) \in R[x]$ such that

$$b^k f(x) = q(x)g(x) + r(x), \text{ with } \deg r(x) < \deg g(x).$$

If b is not a zero divisor in R, then $q(x)$ & $r(x)$ are unique. If $b \in \mathcal{U}(R)$ we may take $k = 0$.

Pf: If $\deg f(x) < \deg g(x)$ we may take $k=0$, $q(x)=0$, and $r(x)=f(x)$. Thus, assume that $\deg f(x) = m \geq \deg g(x) = n$, and $f(x) = a_0 + a_1 x + \dots + a_m x^m$, $g(x) = b_0 + b_1 x + \dots + b_n x^n$, and set $a := a_m$ and $b := b_n$ for clarity.

Induct on m. Base case trivial.

Assume it's true for polynomials of degree $< m$.

Set $f_1(x) = b f(x) - a x^{m-n} g(x)$.

Clearly, $\deg f_1(x) < m$, so we may write

$$b^{k-1} f_1(x) = p(x) g(x) + r(x) \quad \text{where } k-1 \geq 0, \quad p(x), r(x) \in R[x], \quad \deg r(x) < \deg g(x).$$

$$\begin{aligned} b^k f(x) = b^{k-1} b f(x) &= b^{k-1}\left(a x^{m-n} g(x) + f_1(x)\right) \\ &= b^{k-1} a x^{m-n} g(x) + b^{k-1} f_1(x) \\ &= b^{k-1} a x^{m-n} g(x) + p(x) g(x) + r(x) \\ &= \underbrace{\left(b^{k-1} a x^{m-n} + p(x)\right)}_{\text{Call this } q(x).} g(x) + r(x) \quad \checkmark \end{aligned}$$

Next, suppose b is not a zero divisor, and

$$b^k f(x) = q(x) g(x) + r(x), \text{ and}$$
$$b^k f(x) = q_1(x) g(x) + r_1(x). \quad \text{with } \deg r(x), r_1(x) < \deg g(x).$$

Then, $\left(q(x) - q_1(x)\right) g(x) = r_1(x) - r(x)$.

If $q(x) \neq q_1(x)$, then the LHS has degree $\geq n$, since the leading coeff. of $g(x)$ is b (not a zero divisor).

However, the RHS has degree $< n < m$.

Thus, $q(x) = q_1(x)$, and $r(x) = r_1(x)$. ✓

Finally, if $b \in U(R)$, multiply thru by b^{-k}, and replace $q(x)$ & $r(x)$ by $b^{-k} q(x)$ & $b^{-k} r(x)$, resp. ✓ $\square$

The polynomials $q(x)$ and $r(x)$ are called the <u>quotient</u> and <u>remainder</u>.

The division algorithm also holds when R is not comm, as long as b is a unit.

* Henceforth, R is assumed to be commutative with 1.

<u>Thm 2.4</u>: (Substitution). Suppose R, S comm. rings with 1, that $\theta : R \longrightarrow S$ is a homom. with $\theta(1_R) = 1_S$ and $a \in S$. Then $\exists !$ homom $E_a : R[x] \longrightarrow S$ s.t

$$\begin{tikzcd} R \arrow[rr, hook, "\phi"] \arrow[dr, "\theta"'] & & R[x] \arrow[dl, dashed, "E_a"] \\ & S & \end{tikzcd}$$

(i) $E_a(r) = \theta(r)$ $\forall r \in R$

(ii) $E_a(x) = a$.

"Maps $f(x)$ to $f(a)$"

<u>Pf</u>: It is easy to show that E_a is a homom if $E_a(r) = \theta(r)$.

<u>Uniqueness</u>: Suppose $F : R[x] \longrightarrow S$ is a homom with $F(r) = \theta(r)$ $\forall r \in R$ and $F(x) = a$. Then

$$\begin{aligned} F(f(x)) = F(r_0 + r_1 x + \cdots + r_n x^n) &= F(r_0) + F(r_1)F(x) + \cdots + F(r_n)F(x^n) \\ &= \theta(r_0) + \theta(r_1) a + \cdots + \theta(r_n) a^n \\ &= E_a(f(x)) \checkmark \end{aligned}$$

$\square$

<u>Examples</u>:

$$\begin{tikzcd} \mathbb{Z} \arrow[r, hook, "\phi"] \arrow[dr, "\theta"'] & \mathbb{Z}[x] \arrow[d, dashed, "E_{\sqrt{2}}"] \\ & \mathbb{R} \end{tikzcd}$$

$E_{\sqrt{2}} : f(x) \longmapsto f(\sqrt{2})$.

Image is the subring $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$ <u>generated</u> by elts $a + b\sqrt{2}$ for $a, b \in \mathbb{Z}$.

<u>Note</u>: $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ (why?)

$$\begin{tikzcd} \mathbb{Z} \arrow[r, hook, "\phi"] \arrow[dr, "\theta"'] & \mathbb{Z}[x] \arrow[d, dashed, "E_i"] \\ & \mathbb{C} \end{tikzcd}$$

$E_i : f(x) \longmapsto f(i)$.

Image is the subring $\mathbb{Z}[i] \subseteq \mathbb{C}$; all elts of the form $a + bi$ for $a, b \in \mathbb{Z}$ (called the <u>Gaussian integers</u>).

The map E_a is called the <u>evaluation map</u> at a.

<u>Note</u>: θ need not be an injection, but in practice, it is usually the canonical inclusion map. In this case, $E_a(f(x)) = r_0 + r_1 a + \cdots + r_n a^n$, which we call $f(a)$, and we write the image as $R[a] = \{f(a) : f(x) \in R[x]\}$.

<u>Prop 2.5</u> (Remainder theorem). Suppose R is comm. with 1, $f(x) \in R[x]$, and $a \in R$. Then the remainder of $f(x)$ divided by $g(x) = x - a$ is $r = f(a)$.

<u>Pf</u>. Write $f(x) = q(x)(x-a) + r$. Substitute a for x to get $f(a) = q(a)(a-a) + r = r$.

$\square$

6

<u>Cor</u>: (Factor theorem): Suppose R is comm. with 1, $f(x) \in R[x]$, $a \in R$ and $f(a)=0$. Then $x-a$ is a factor of $f(x)$, i.e., $f(x) = g(x)(x-a)$ for some $g(x) \in R[x]$.

<u>Def</u>: If R & S are comm. rings with $R \subseteq S$, $1_R = 1_S$, then an elt. $a \in S$ is <u>algebraic</u> over R if $f(a)=0$ for some non-zero polynomial $f(x) \in R[x]$. If $a \in S$ is not algebraic over R, it is <u>transcendental</u> over R.

<u>Note</u>: $a \in S$ is algebraic over R iff E_a is not 1-1.

<u>Example</u>: • $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Z}$ since $f(\sqrt{2})=0$ for
• $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Z}$.

If R is an integral domain, then the field of fractions of $R[x]$ is the field of <u>rational functions</u> over R:

$$R(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in R(x), \ g(x) \neq 0 \right\}.$$

<u>Polynomials in several indeterminates.</u>

Let $I = \{0,1,2,3,\dots\}$ and consider $I^n = I \times \dots \times I$ (n copies).
Let R be a ring, and define

$$P_n(R) = \{a : I^n \longrightarrow R : a(x)=0 \text{ all but finitely many } x \in I^n\}.$$

<u>Note</u>: If $n=1$, then $P_1(R) = P(R)$.

Write 0 for $(0,0,\dots,0) \in I^n$ and if $i = (i_1, i_2, \dots, i_n) \in I^n$ and $j = (j_1, j_2, \dots, j_n) \in I^n$, define

$$i+j = (i_1+j_1, i_2+j_2, \dots, i_n+j_n) \in I^n.$$

Define addition & mult. on $P_n(R)$ as follows:

$$(a+b)(i) = a(i) + b(i)$$
$$(ab)(i) = \sum \{ a(j)b(k) : j,k \in I^n,\ j+k = i \}$$

Informally, think of an elt of I^n as corresponding to a monomial. e.g., $a(0,3,4) = -6 \longleftrightarrow -6x_1^0 x_2^3 x_3^4$, and a function in $P_n(R)$ as assigning coefficients to monomials.

<u>Thm 2.6</u>: If R is a ring, then $P_n(R)$ is a ring, and $P_n(R)$ is comm. iff R is, and has 1 iff R has 1.

<u>Pf</u>: Exercise (straightforward, but tedious).

<u>Note</u>. The identity function $1 \in P_n(R)$ is the function $1 : I^n \longrightarrow R$, where $1(0) = 1 \in R$, $1(i) = 0 \in R$ if $0 \neq i \in I^n$. (Secretly, assigns coeff. 1 to $x_1^0 x_2^0 \cdots x_n^0$, 0 otherwise).

For each $r \in R$, define a function $a_r \in P_n(R)$:

$$a_r(0) = r, \quad a_r(i) = 0 \quad \text{if } 0 \neq i \in I^n.$$

Then, $a_r + a_s = a_{r+s}$ and $a_r a_s = a_{rs}$.

So, the map $r \longmapsto a_r$ (Secretly, $r \mapsto r x_1^0 x_2^0 \cdots x_n^0$) is 1-1.

Thus, we may identify r with $a_r \in P_n(R)$, and view R as a subring of $P_n(R)$.

Let R be a ring with 1, let $e_k = (0,0,\ldots,0,\underset{\text{pos } k}{1},0,\ldots,0)$

Define $X_k \in P_n(R)$: $X_k(e_k) = 1$, $X_k(i) = 0$ $e_k \neq i \in I^n$.

Often, if $n=2,3$, write $X_1 = x$, $X_2 = y$, $X_3 = z$.

Note: $X_k^2(2e_k) = 1$, $X_k^2(i) = 0$ $i \neq 2e_k$, and in general,
$X_k^m(me_k) = 1$, $X_k^m(i) = 0$ $i \neq me_k$ for $1 \le m \in \mathbb{Z}$.

(secretly, e.g., $(0,3,0) \longmapsto 1 X_1^0 X_2^3 X_3^0 = 1 X_2^3$).

Note: $X_i X_j = X_j X_i$ (i.e, these commute as functions, $I^n \to R$).

For any $i \in (i_1, \dots, i_n) \in I^n$ and $r \in R$, consider $r X_1^{i_1} \cdots X_n^{i_n} \in P_n(R)$, which has value r at $i \in I^n$ and 0 elsewhere, i.e, has one-point support.

Since any $a \in P_n(R)$ can be written uniquely using functions with one-point support, each $0 \neq a \in P_n(R)$ can be written uniquely as a sum of elts of the form $r X_1^{i_1} \cdots X_n^{i_n}$, called monomials.

Say that the degree of $a = r X_1^{i_1} \cdots X_n^{i_n}$ is $\deg a = i_1 + \cdots + i_n$.
If a is a sum of monomials $a = a_1 + \cdots + a_m$, then say $\deg a = \max\{\deg a_i : 1 \le i \le m\}$.

Also, say that $\deg 0 = -\infty$, and if all a_i's have the same degree, call $a \in P_n(R)$ homogeneous.

The elements of $P_n(R)$ are called polynomials in the n commuting indeterminates $X_1, \dots, X_n$.

We write $R[X_1, \dots, X_n]$ for $P_n(R)$ and denote elements by $f(X_1, \dots, X_n)$, etc.
Often, we write X for $(X_1, \dots, X_n)$ and thus $f(X)$ for $f(X_1, \dots, X_n)$.

Prop 2.7: Let R be a ring with 1 and $f(x), g(x) \in R[x_1, \dots, x_n]$.

Then: (a) $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$, and

(b) $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$.

Moreover, equality holds in (b) if R has no zero divisors.

Thm 2.8 (Substitution). Let R, S be comm. rings with 1, and $\theta : R \longrightarrow S$ a homom with $\theta(1_R) = 1_S$. If $a_1, \dots, a_n \in S$, then $\exists!$ homom

$E = E_{(a_1, \dots, a_n)} : R[x_1, \dots, x_n] \longrightarrow S$

s.t. (i) $E(r) = \theta(r) \quad \forall r \in R$

(ii) $E(x_i) = a_i \quad 1 \leq i \leq n$

$$\begin{tikzcd} R \arrow[r, hook, "\Phi"] \arrow[dr, "\theta"'] & R[x_1, \dots, x_n] \arrow[d, dashed, "E_{(a_1, \dots, a_n)}"] \\ & S \end{tikzcd}$$

Pf: Define $E(r x_1^{i_1} \cdots x_n^{i_n}) = \theta(r) a_1^{i_1} \cdots a_n^{i_n}$ for monomials, & extend to polynomials in the obvious way. Check this works. $\square$

Note: We could have defined $R[x_1, \dots, x_n]$ abstractly using this universal mapping property.

Another construction: Define $R[x_1, x_2] = (R[x_1])[x_2]$, etc.

We could extend this to an arbitrary index set as well, i.e, define $R[x_\alpha : \alpha \in A]$.

If θ is injective, then the homom E "substitutes" elements from S in place of the x_i's, by $f(x_1, \dots, x_n) \overset{E}{\longmapsto} f(a_1, \dots, a_n)$ where $a_i \in S$.

The image is a subring of S, denoted $R[a_1, \dots, a_n]$.

Example:

$$\begin{tikzcd} \mathbb{Z} \arrow[rr, hook] \arrow[dr] & & \mathbb{Z}[x,y] \arrow[dl, "E_{(\sqrt{3},\sqrt{5})}"] \\ & \mathbb{R} & \end{tikzcd}$$

$$\operatorname{Im}(E) = \mathbb{Z}[\sqrt{3}, \sqrt{5}] = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} : a,b,c,d \in \mathbb{Z}\}$$

Def: Elements $a_1, \dots, a_n \in S$ are <u>algebraically dependent</u> over R if $f(a_1, \dots, a_n) = 0$ for some $0 \neq f(X) \in R[X_1, \dots, X_n]$.

Otherwise, they are <u>algebraically independent</u> over R.

Ex: (1) $a_1 = \sqrt{3}$, $a_2 = \sqrt{3}$ are algebraically dependent over $\mathbb{Z}$

Consider $f(x,y) = (x^2-3)(y^2-5)$

(2) $a_1 = \sqrt{\pi}$, $a_2 = 2\pi + 1$ are algebraically dependent over $\mathbb{Z}$.

Consider $f(x,y) = 2x^2 - y + 1$

(3) It is unknown whether $a_1 = \pi$, $a_2 = e$ are algebraically dependent over $\mathbb{Z}$.

Note: • $a \in S$ algebraically indep. over $R \iff a$ transcendental over R.

• $a_1, \dots, a_n$ alg. indep. over $R \implies$ all a_i transcendental over R.

"$\Longleftarrow$" fails (see Ex (2) above).

Usually, we omit X_i^0, so $R[X_1] \subseteq R[X_1, X_2] \subseteq R[X_1, X_2, X_3] \subseteq \cdots$, and write $R[X_1, X_2, X_3, \dots] := \bigcup \{R[X_1, \dots, X_k] : 1 \leq k \in \mathbb{Z}\}$.

If R is an integral domain, then the field of fractions of $R[X_1, \dots, X_n]$ are the <u>rational functions</u> denoted $R(X_1, \dots, X_n)$:

$$\left\{ \frac{f(X_1, \dots, X_n)}{g(X_1, \dots, X_n)},\quad g(X_1, \dots, X_n) \neq 0,\quad f(X), g(X) \in R[X_1, \dots, X_n] \right\}.$$